

presented by



Microsoft



Overview of Windows 10 Requirements for TPM, HVCI and SecureBoot

UEFI Spring Plugfest – May 18-22, 2015

Gabe Stocco, Scott Anderson, Suhas Manangi

Agenda



- Introduction
 - TPM
 - Device Guard and HVCI
 - Secure Boot
 - Few other important things
- Q&A



TPM (Trusted Platform Module)

TPM



- New features enabled by a properly configured TPM
 - Windows Hello (Passwordless, secure, login)
 - Remote Health Attestation
 - Virtual Smart Card

TPM



- TPM 2.0
 - Required on Mobile at RTM
 - Required on Client if either:
 - Silicon on device has fTPM support.
 - 365 days have elapsed since RTM of Win10.
 - HLK Tests available
- Important Notes Regarding Client
 - Clients may ship with more than one TPM.
 - Windows only supports one TPM.
 - When more than one TPM is available a toggle is needed.
 - Warn user that they should disable Bitlocker before changing TPMs and that they will lose any stored keys.
- Correct TPM PCR value measurement and validation are critical.

TPM



- HMAC Commands are needed
 - Essential for new features – such as Windows Passport/Hello
- TPM Must be able to be disabled.
 - See Min HW Requirement for specific procedure to follow to ensure TPM is fully disabled.
- These new requirements set up Windows to be a highly secure by default platform, providing high security scenarios out of the box.



Device Guard and HVCI



Device Guard Overview

The Parts of the solution



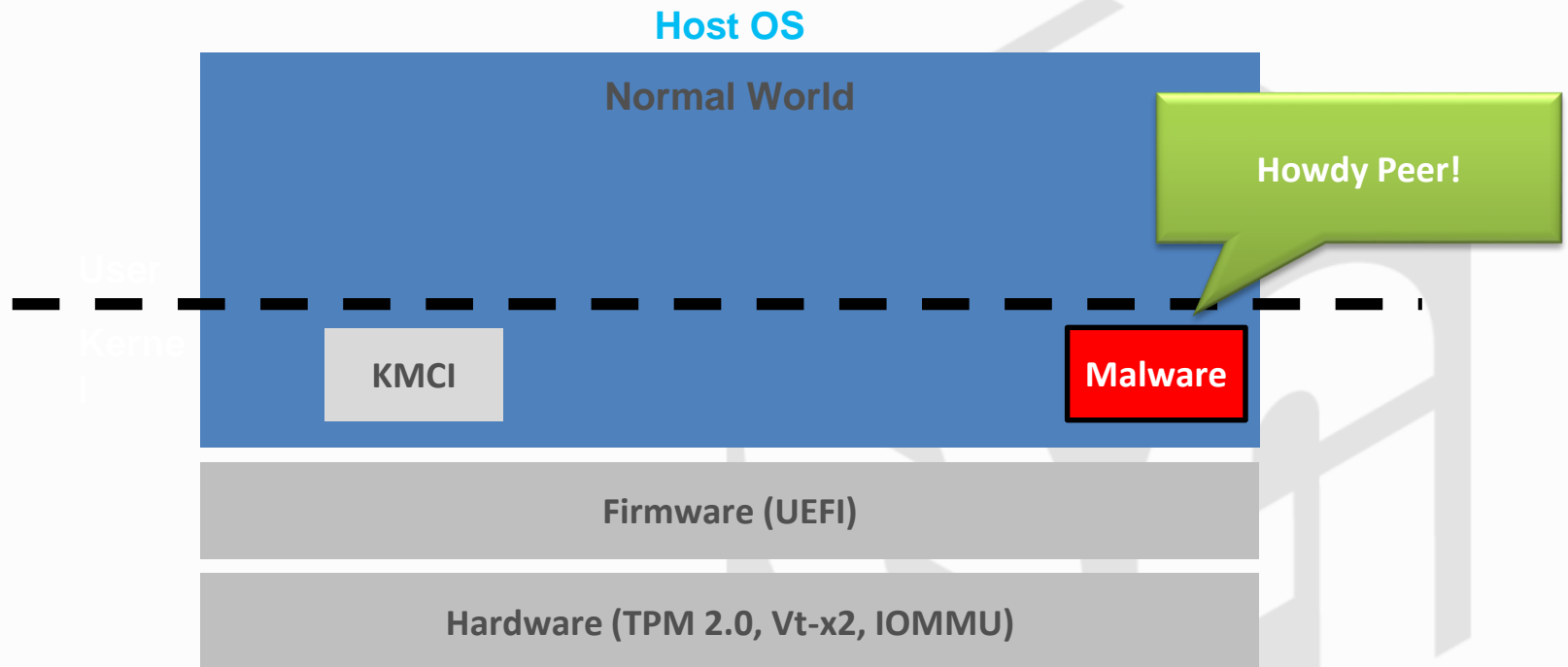
- Hardware security
- Configurable code integrity
- Virtualization based security
- Protects critical parts of the OS against admin/kernel level malware
- Manageability via GP, MDM, or PowerShell

Virtualization Based Security



- Provides a new trust boundary for system software
 - Leverage platform virtualization to enhance platform security
 - Limit access to high-value security assets from supervisor mode (CPL0) code
- Provides a secure execution environment to enable:
 - Protected storage and management of platform security assets
 - Enhanced OS protection against attacks (including attacks from kernel-mode)
 - A basis for strengthening protections of guest VM secrets from the host OS
- Windows 10 services protected with virtualization based security
 - LSA Credential Isolation
 - vTPM (server only)
 - Kernel Mode Code Integrity (HVCI)

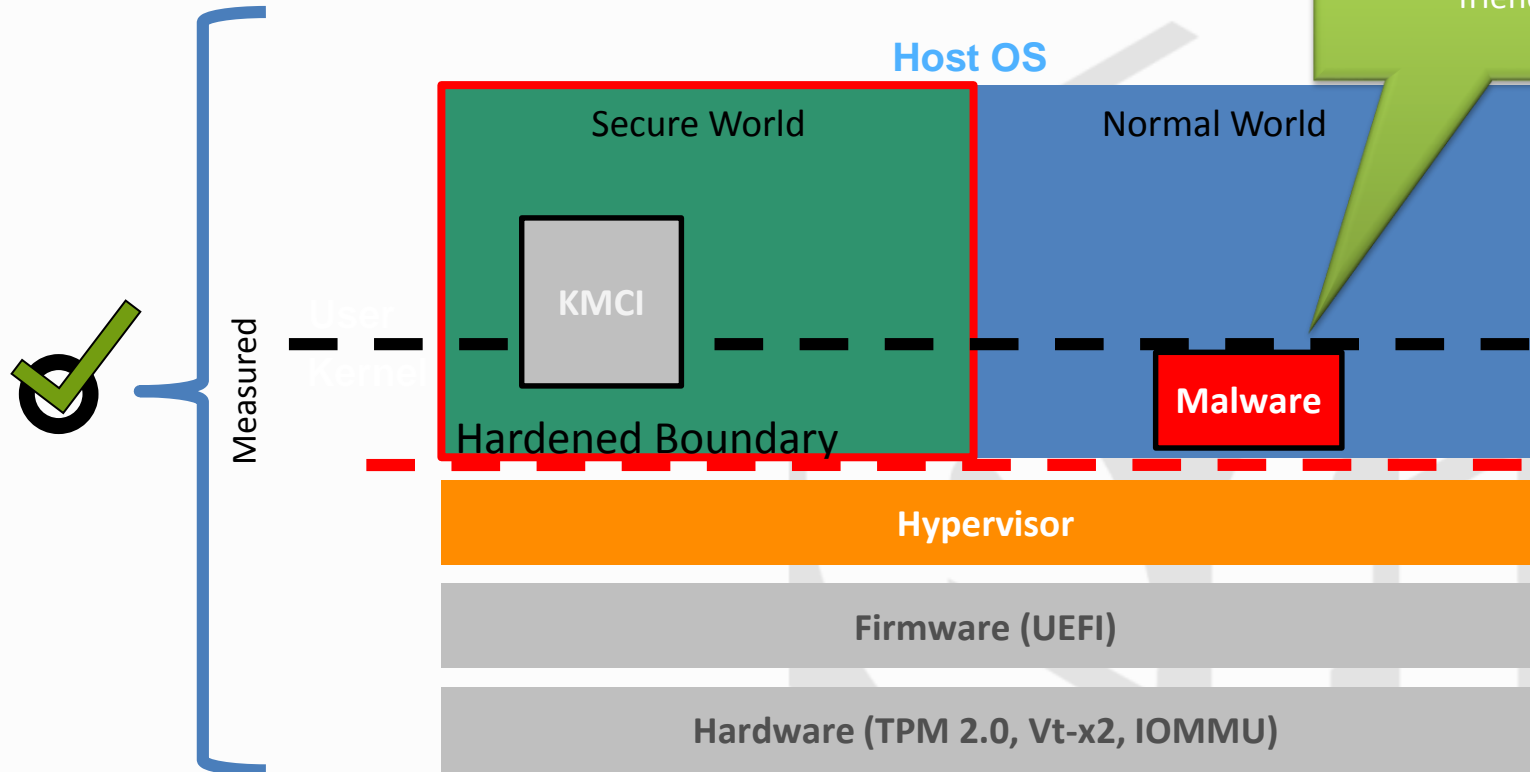
KMCI in Windows 8.1



KMCI with Windows 10 VBS



I thought we could be friends ☹️



HVCI



- CI rules are still enforced even if a vulnerability allows unauthorized kernel mode memory access
- Memory pages are only marked executable if CI validation succeeds
- Kernel memory cannot be marked both writable and executable
- BUT impacts
 - Driver compatibility
 - UEFI Runtime services compatibility

Hardware Security



- This means the users physically in possession of a machine cannot easily modify it
- Includes:
 - Platform Secure Boot
 - Secure Firmware Updates
 - Locking the BIOS menus
 - Restricting Boot options

Device Guard and HVCI Ready Devices



- Virtualization extensions ON by default
- UEFI Runtime services compatible with HVCI
- BIOS locked down against Physical attacker
 - Boot options
 - Secure Boot
 - Secure Firmware Updates



Secure Boot



Secure Boot



- HSTI – Required for Win10 (Mobile SKU and CS)
 - Specification published on msdn
 - HLK test available
- Microsoft UEFI CA - Required for Win10
 - DBX must ship upto date
 - HLK test for default DBX available

HSTI



- HSTI is a Hardware Security Testability Interface
 - Required by System.Fundamentals.Firmware.CS.UEFISecureBoot.Provisioning
 - On MSDN here: <https://msdn.microsoft.com/en-us/library/windows/hardware/dn879006.aspx>
 - HSTI is an interface to report the results of security-related self-tests.
 - IHVs provide the definition of the reporting fields.
 - Each reporting entity is responsible for full analysis and testing of their own components.
- HSTI is for providing high assurance validation of proper security configuration as systems leave the line.
 - This reduces support load for IBVs, decreases debug time for OEMs and increases consumer confidence in properly configured machines.

Microsoft UEFI CA – signing service



Policy details: [msdn link](#)

1. No organization only, OEM only, internal tools only products – only 3rd party products that supported to be run on all UEFI machines in the world
2. RTM product only
3. No products that would possibly bypass Secure Boot, hence the need for detailed security review and resulting turn around time

NOTE: Brainstorm and discussion session



Few other important things



Remote Attestation



Remote Attestation: is part of New “Host Guardian Service” Windows Server Role

- Validate host identity & host configuration
- Issue Attestation Certificate to a validated host

Host Validation:

- Host Identity validation:
 - Known good TPM’s EKpub
- Host Configuration validation:
 - Known good TPM measurements
 - Consistent TCG log
 - Known good HVCI policy hash
- Host UEFI validation:
 - Known good DB & DBX



Remote Attestation - UEFI Requirements



Windows 10 Server Assurance AQ requirements:

TPM 2.0

- **Mandatory:** TPM 2.0 is required
- **Mandatory:** TPM Functionality required as specified in System.Fundamentals.TPM20 requirements for Windows 10
- **Mandatory:** An automated tool is provided to clear TPMs remotely on an arbitrary number of managed machines.
- **Optional:** PPI clear settings may be chosen by the OEM.
- **Optional:** An automated tool is provided to toggle PPI status remotely on an arbitrary number of managed machines.

UEFI Secure Boot

- **Mandatory:** Secure Boot requirements as specified in System.Fundamentals.Firmware.UEFISecureBoot for Windows 10.
- **Mandatory:** Secure Boot is shipped enabled or an automated tool is provided to enable Secure Boot remotely managing arbitrary number of machines.

Recommendations on UEFI 2.5 updates



1. **Mantis 1224: Physical Memory Protection attribute**
(MemoryProtectionAttribute)
 - Needed for HVCI on Windows 10.
2. **Mantis 1227: Platform Recovery**
 - Recommended to not implement this until at least one OS adopts.
 - Windows 10 doesn't have a support for this and hopeful to have support in the next OS release
3. **Mantis 1263: Customized Deployment of Secure Boot**
 - Recommended to not implement this until at least one OS adopts.
 - Windows 10 doesn't have a support for this and hopeful to have support in the next OS release

Firmware Update through WU



Open to all OEMs

- UEFI Plugfest 2014 presentation:

[Leveraging Windows Update to Distribute Firmware ...](#)

[www.uefi.org/sites/default/files/resources/2014 UEFI Plugfest 07](http://www.uefi.org/sites/default/files/resources/2014_UEFI_Plugfest_07)

...

MSDN documentation:

<http://www.microsoft.com/en-us/download/details.aspx?id=38405>

Interested? Follow-up with david.edfeldt@microsoft.com and Dave.Roth@microsoft.com>

Q & A



Thanks for attending the
UEFI Spring Plugfest 2015



For more information on
the Unified EFI Forum and
UEFI Specifications, visit
<http://www.uefi.org>

presented by

